DAHAM DILESH NANAYAKKARA

Colombo, Sri Lanka | +94 750 936 434 |https://github.com/dilesh591 |dahamdilesh@gmail.com |
https://dahamdilesh-portfolio.netlify.app/ |Linkdin.com

PROFESSIONAL SUMMARY

Final-year Computer Science student with a focus on Software Engineering and Cybersecurity Operations. Developer of automated security solutions including a malware triage tool that reduced analysis time by 95%. Skilled in SIEM platforms (Splunk, Sentinel) , Python automation , and threat mapping via MITRE ATT&CK. Seeking a SOC Analyst internship to apply hands-on experience in incident response and alert triage.

EDUCATION

Royal Collage 2011 – 2023
Colombo 07

BSc (Hons) Computer Science - Software Engineering Specialization 2023-2027
University of Wolverhampton (offered by CINEC Campus) *Colombo, Sri Lanka*

Cyber Security & Networking Certificate 2026 Jan -2026 may
Institute Of Information Technology (IIT) *Colombo, Sri Lanka*

TECHNICAL SKILLS

Programming Languages: Python (Primary), Java, C, C++, SQL, Bash Scripting, HTML, CSS
Security Tools: Splunk, Microsoft Defender for Endpoint, Microsoft Sentinel, Wireshark, Nmap, Windows PowerShell, Linux CLI
Frameworks & Standards: OWASP Top 10, MITRE ATT&CK, NIST Cybersecurity Framework, ISO 27001, ISO 42001
Competencies: SIEM Analysis, Incident Response, Malware Analysis, Network Monitoring, Threat Intelligence, Vulnerability Assessment, Security Documentation, Risk Assessment

TECHNICAL PROJECTS

Automated Malware Analysis & Threat Detection Platform Python, Flask, Ghidra, HTML/CSS/JavaScript

- Developed lightweight malware triage tool using Python and Ghidra reverse engineering framework to automate SOC malware analysis workflow, reducing investigation time from 2+ hours to 5 minutes per sample
- Implemented threat detection engine identifying 15+ suspicious behavioral patterns including process injection (VirtualAllocEx, WriteProcessMemory), registry modification, credential theft, and command execution techniques
- Built all-in-one web application with embedded frontend enabling drag-and-drop binary upload, real-time analysis monitoring, and comprehensive reporting with IOC extraction (MD5/SHA1/SHA256 hashes, suspicious APIs, malicious strings)

AI-Assisted SOC Decision Support System (third party contributor) Python, Ollama, MITRE ATT&CK

- Developed an intelligent alert triage system using Python and local AI (Ollama) to reduce false positive alerts in SOC operations

- Implemented explainable reasoning capabilities aligned with MITRE ATT&CK framework for threat categorization

- Enhanced analyst efficiency by automating initial alert assessment while preserving critical security detections

Student Management System Java, MySQL, Spring Boot, JUnit 5, JDBC

- Designed a 3-tier system using the DAO pattern and JDBC to decouple business logic from the MySQL persistence layer, ensuring 100% data integrity.

- Engineered a RESTful Web Service with Spring Boot to expose secure HTTP endpoints, facilitating seamless data exchange via JSON payloads.

- Developed standardized administrative modules by implementing Java Interfaces and OOD principles, streamlining entity lifecycles for students and faculty.

- Optimized software reliability by authoring a comprehensive JUnit 5 test suite, achieving high code coverage for core business logic and database operations.

CERTIFICATIONS & TRAINING

Google Cybersecurity Professional Certificate (2025)

- Gained hands-on experience in SOC operations, threat detection, and incident response using real-world security scenarios
- Learned SIEM fundamentals, log analysis, network security, and risk management aligned with NIST Cybersecurity Framework
- Applied MITRE ATT&CK, OWASP Top 10, and basic Python automation for security analysis
- Tools & platforms: Splunk, Wireshark, Linux CLI, SQL, Python

Cyber Security & Networking Certificate – Institute of Information Technology (IIT)

- Developed strong foundations in network security, TCP/IP, routing & switching, and secure network design
- Performed network traffic analysis, packet inspection, and vulnerability identification
- Hands-on practice with firewalls, IDS/IPS concepts, and basic penetration testing techniques
- Tools: Wireshark, Nmap, Linux, Windows networking utilities

Splunk Academy – Fundamentals & Junior Analyst Certificates

- Built practical expertise in SIEM log ingestion, search processing language (SPL), and dashboard creation
- Conducted security event correlation, alert triage, and incident investigation using real datasets
- Learned SOC workflows including threat detection, IOC analysis, and security reporting
- Tools: Splunk Enterprise, SPL, Security dashboards, Log sources (Windows, Network, Auth logs)

AWS Cloud Practitioner Essentials

- Acquired foundational knowledge of cloud security, shared responsibility model, and AWS core services
- Learned cloud identity, access management, and monitoring concepts relevant to security operations
- Understood secure cloud architectures and compliance basics
- Services covered: IAM, EC2, S3, CloudWatch, VPC, AWS security best practices

INFOSEC – Malware Analysis Introduction

- Learned core malware analysis techniques including static and basic dynamic analysis
- Analyzed malicious binaries to identify suspicious APIs, strings, hashes, and behavioral indicators
- Built understanding of Windows internals, malware execution flow, and IOC extraction
- Tools: Ghidra, PE analysis tools, Strings, Hashing utilities, Sandbox concepts

In Progress: ISC2 Certified in Cybersecurity (CC), CompTIA Security, Microsoft Certified: Security, Compliance, and Identity Fundamentals

REFERENCES

Maduwanthi Kiriwandarage
Deputy Head of the Department / Senior Lecturer
Department of Information Technology
Faculty of Computing, CINEC Campus
Email: maduwanthi.uthpala@cinec.edu
Phone: +94 77 612 2034

Eshandi Aththanayaka
Lecturer in information technology
Department of Information Technology
Faculty of Computing, CINEC Campus
Email: eshandi.amr@cinec.edu
Phone: +94 71 096 0601